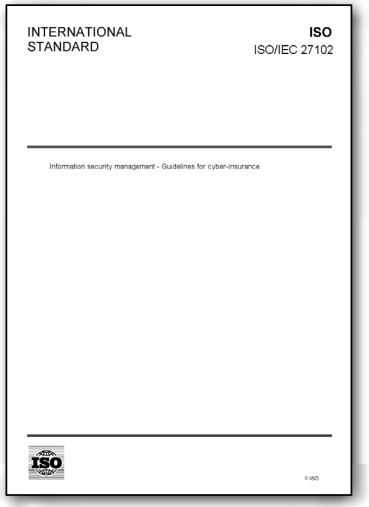
Aktuální normy a publikace o bezpečnosti



Pojištění kybernetických rizik

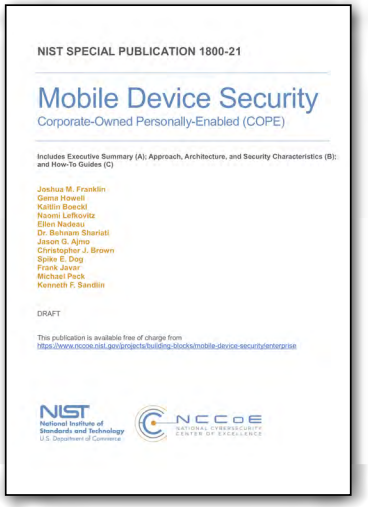
Srpnovým přírůstkem do rodiny norem *ISO 27k je ISO/IEC 27102:2019 – Information security management – Guidelines for cyber-insurance*. Standard se věnuje pojištění kybernetických rizik. Poskytuje doporučení pro organizace, které jako jednu z možností zvládání kybernetických bezpečnostních rizik zvažují nákup kybernetického pojištění. Vysvětluje základní koncepty a přístupy k tomuto typu pojištění, jaká jsou obvyklá očekávání ze strany zákazníků a pojišťoven, výhody a možná omezení pro tento typ pojištění, jak co nejlépe nastavit pojištění odpovědnosti pro manažery a zaměstnance. Dává doporučení pro sdílení dat a informací mezi pojištěným a pojistitelem. Pro agenty pojišťovacích ústavů vysvětluje základní principy kybernetické bezpečnosti.

https://www.iso.org/

Správa osobních údajů

Druhým srpnový standardem je *ISO/IEC 27701:2019 – Information technology – Security techniques – Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management – Requirements and guidelines*. Dokument specifikuje požadavky a poskytuje doporučení pro zřízení, implementaci, údržbu a neustálé zlepšování systému řízení ochrany osobních údajů (PIMS, Privacy Information Management System) ve formě rozšíření ISO/IEC 27001 a ISO/IEC 27002. Obsahuje specifické požadavky k jednotlivým krokům PDCA cyklu ISO/IEC 27001, doporučení pro implementaci opatření ISO/IEC 27002, dodatečná doporučení pro správce a zpracovatele osobních údajů. Standard také obsahuje mapování na ISO/IEC 29100 a ISO/IEC 27108.

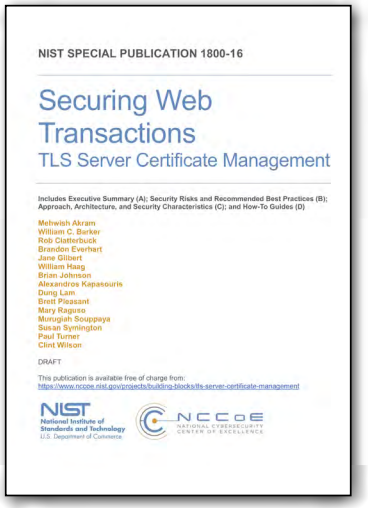
https://www.iso.org/



Zabezpečení mobilních zařízení

Americké centrum pro kybernetickou bezpečnost NCCoE ve spolupráci s NIST připravilo návrh standardu *SP 1800-21 (DRAFT) Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, který cílí na zabezpečení mobilních zařízení využívaných ve firemním prostředí. Ukazuje, jak mohou organizace používat přístup založený na standardech a komerčně dostupných technologiích k zajištění svých bezpečnostních potřeb při používání mobilních zařízení pro přístup k podnikovým zdrojům. Obsahuje příklad identifikace a hodnocení rizik použití mobilních zařízení ve fiktivní organizaci. Pro jednotlivé hrozby identifikované v případové analýze je uveden výčet doporučených opatření pro jejich mitigaci. Další část pak nabízí doporučení pro instalaci, konfiguraci a integrace vybraných řešení pro správu mobilních zařízení.

https://csrc.nist.gov/publications/sp800



Zabezpečení www komunikace

SP 1800-16 (DRAFT) Securing Web Transactions: TLS Server Certificate Management ukazuje velkým a středním podnikům, jak zavést a provozovat systém správy TLS (Transport Layer Security) certifikátů, jak se vyhnout rizikům spojeným s provozem a chybnou konfigurací. Popisuje obvyklé problémy, kterým organizace při správě TLS certifikátů čelí (např. expirované certifikáty, rychlou výměnu velkého počtu certifikátů v reakci na kompromitaci certifikační autority nebo nové zranitelnosti). Poskytuje doporučení a postupy pro správu velkého počtu certifikátů. Popisuje případovou implementaci, která ukazuje jak předcházet, detekovat a reagovat na incidenty související s certifikáty. Poskytuje mapování doporučených postupů pro správu TLS certifikátů na NIST Cybersecurity Framework (rámec pro zvyšování úrovně kybernetické bezpečnosti).

https://csrc.nist.gov/publications/sp800

Ing. Libor Široký, CISM, CRISC, AMBCI, *siroky@rac.cz*